AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

Claim 1 (Previously Presented): A method for enabling secure communication between a client on an open network and a server apparatus on a secure network, the method performed on an intermediary apparatus coupled to the secure network and the open network, comprising:

negotiating a secure communications session with the client apparatus via the open network;

negotiating an open communications session with the server via the secure network;

receiving encrypted packet application data for a security record spanning multiple data packets, wherein the security record has a length greater than a packet length associated with the multiple data packets;

decrypting the encrypted packet application data in each data packet;

forwarding decrypted, unauthenticated application data to the server via the secure network;

discarding at least a portion of the decrypted, unauthenticated packet application data for the security record prior to receiving a final packet of the security record; and

authenticating the security record on receipt of the final packet of the security record.

Claim 2 (Previously Presented): The method of claim 1 wherein forwarding includes:

forwarding data which spans over multiple TCP segments.

Claim 3 (Cancelled).

Claim 4 (Currently Amended): The method of claim 1

wherein only a remaining portion of the packet application data for the security record is buffered as a minimal length sufficient to complete a block cipher used to encrypt the data.

Claim 5 (Previously Presented): The method of claim 1 wherein authenticating includes authenticating the decrypted data for the security record upon receiving a final TCP segment of a multi-segment encrypted data stream and after forwarding the decrypted, unauthenticated application data received prior to the final TCP segment.

Claim 6 (Previously Presented): The method of claim 1 further including, after forwarding the decrypted, unauthenticated application data to the server, notifying the client apparatus if a failure in authenticating the security record occurs.

Claim 7 (Currently Amended): A method for processing encrypted data transferred between a first system and a second system, comprising:

providing an accelerator device including a decryption engine in communication with the first system via an open network and the second system via a secure network;

receiving encrypted data from the first system via the open network in the form of application data spanning multiple packets, wherein a last packet of the multiple packets includes information for authenticating the application data;

decrypting the application data contained within the multiple packets as the multiple packets are received;

forwarding the decrypted application data as the multiple packets are decrypted to the second device via the secure network;

buffering a portion of the decrypted application data and discarding a remaining portion prior to authentication of the application data; and

authenticating the application data when the information for authenticating the application data is received in the last of the multiple packets.

Claim 8 (Previously Presented): The method of claim 7 wherein receiving comprises receiving SSL encrypted data.

Claim 9 (Previously Presented): The method of claim 7 wherein decrypting comprises decrypting application data encrypted using SSL and a DES algorithm.

Claims 10-11 (Cancelled)

Claim 12 (Currently Amended): The method of claim 7 wherein buffering comprises buffering the application data for a minimal length less than a security record but sufficient to complete a block cipher used to encrypt the data.

Claim 13 (Original): The method of claim 12 wherein said block cipher is a form of DES.

Claim 14 (Previously Presented): The method of claim 7 wherein authenticating includes alerting the first device if authenticating fails after forwarding the decrypted, unauthenticated application data that is received prior to the last one of the multiple packets.

Claim 15 (Previously Presented): The method of claim 7 wherein authenticating includes generating a reset to the second device if said authenticating fails.

Claim 16 (Previously Presented): A method of providing secure communications using limited buffer memory in a processing device, comprising:

receiving encrypted data having a length greater than a TCP segment carrying said data;

buffering the encrypted data in a memory buffer in the device, the buffer having a length equivalent to a block cipher size necessary to perform the cipher;

decrypting the buffered segment of the received encrypted data to provide decrypted application data; and

forwarding the decrypted application data to a destination device.

Claim 17 (Original): The method of claim 16 wherein the block cipher is 3DES.

Claim 18 (Original): The method of claim 16 wherein the block cipher is DES.

Claim 19 (Previously Presented): The method of claim 16 further including authenticating the data on receipt of a final segment of the encrypted data after forwarding the unauthenticated application data that is received prior to the final segment.

Claim 20 (Previously Presented): The method of claim 19 further including generating an alert if authenticating results in a failure.